UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/648,644	08/27/2003	Robert Aarts	59643-00295	3885

32294 7590 07/02/2008

SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA, VA 22182-6212

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/02/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/648,644	AARTS ET AL.	
	Examiner	Art Unit	
	JUNG KIM	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the RCE filed on 4/16/08.

2. Claims 1-28 are pending.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/16/08 has been entered.

Response to Arguments

4. Applicant's arguments have been fully considered but they are not persuasive. In particular, applicant alleges that "there is no disclosure nor suggestion in Koike of any method or apparatus wherein a privacy policy and/or usage policy specifies a strictness level which is selected from a defined set of strictness levels, with the strictness levels describing constraints related to the access of data. The configurations of Koike merely disclose individually specified conditions for release of information, according to privacy preference." (Remarks, pg. 14) However, Koike expressly discloses that the data is administered in accordance with P3P standards. (paragraphs 85 and 175) P3P defines

several predefined statements which define strictness levels under the categories purpose, retention and recipient. For example, under the retention category, P3P defines the following elements ordered from most strict to least strict: "no-retention", "stated-purpose", "legal-requirements", "business-practices" and "indefinitely"; under the recipient category, P3P defines the following elements ordered from most strict to least strict: "ours", "delivery", "same", "other-recipient", "unrelated" and "public". Therefore, contrary to applicant's arguments, Koike expressly discloses a privacy policy and/or usage policy that specify a strictness level which is selected from a defined set of strictness levels, with the strictness levels describing constraints related to the access of data. For these reasons, the claims remain rejected under Koike.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-7, 9, 11-14, 16, 18-25 and 27 are rejected under 35 U.S.C. 102(e) as being anticipated by Koike US 2003/0084300 (hereinafter Koike).

7. As per claims 1-7 and 9, Koike discloses a method comprising:

a. receiving at a broker a usage policy for constraints related to data of a user in a communication system; receiving a request for data associated with the user from a service provider in the communication system to the broker, wherein the service provider possesses a privacy policy; checking, in the broker, the request against a usage policy of the user; and deciding whether the data can be released; (paragraphs 84 and 115);

b. wherein the privacy policy and the usage policy specify a strictness level, selected from a defined list of strictness levels, describing the constraints related to the access of data; (figs. 2 and 3, paragraph 85 and 175)

c. further comprising: using the user to define the usage policy for the constraints related to the data; (paragraph 86-89)

d. further comprising: providing the broker with a predefined set of privacy policies and usage policies; (paragraph 89)

e. wherein the providing comprises providing the privacy policies and the usage policies comprising similar information elements; (paragraph 89)

f. wherein the providing comprises providing at least one of the privacy policies and at least one of the usage policies which specify a strictness level describing the constraints related to the data; (paragraphs 85 and 175)

g. further comprising: using the user to choose the usage policies for the constraints related to the data; (paragraphs 86-89)

h. further comprising: releasing user data when the at least one of the privacy policies of the service provider matches with the specified strictness level of the at least one of the usage policies of the user; (paragraphs 117-126)

i. allowing the user to reduce a usage policy requirement when the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage policies of the user (paragraph 127)

8. As per claim 11, Koike discloses a system comprising: a service provider possessing a privacy policy; and a broker hosting a usage policy for constraints related to data of a user, configured to check a request from the service provider against the usage policy of the user and to decide whether data associated with the user can be released in response to the request; wherein the usage policy specify a strictness level, selected from a defined list of strictness levels, describing the constraints related to the access of data. (paragraphs 79-100 and 113-150)

9. As per claim 12, Koike discloses a system, comprising: introducing means for introducing to a broker a usage policy for constraints related to data of a user; receiving means for receiving a request for data associated with the user from a service provider to the broker; checking means for checking, in the broker, the request against a usage policy of the user; and deciding means for deciding whether the data can be released; wherein the usage policy specifies a strictness level, selected from a defined

list of strictness levels, describing the constraints related to the access of data. (paragraphs 79-100 and 113-150)

10. As per claims 13, 14 and 16, Koike discloses an apparatus, comprising: a receiver configured to receive a request for data associated with a user from a service provider; and a processor configured to check the request against a usage policy of the user and to decide whether the data can be released wherein the usage policy specifies a strictness level, selected from a defined list of strictness levels, describing constraints related to the access of data; wherein the processor is further configured to: release user data when at least one privacy policy of the service provider matches with a specified strictness level of the usage policy of the user; wherein the processor is configured to: allow the user to reduce a usage policy requirement when the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage policies of the user. (paragraphs 79-100 and 113-150)

11. As per claim 18, Koike discloses an apparatus, comprising: receiving means for receiving a request for data associated with a user from a service provider; checking means for checking the request against a usage policy of the user; and deciding means for deciding whether the data can be released; wherein the usage policy specifies a strictness level, selected from a defined ordered list of strictness

levels, describing the constraints related to the access of data. (paragraphs 79-100 and 113-150).

12. As per claims 19-25 and 27, Koike discloses a computer-readable medium comprising computer-executable components the components configured to: receive a usage policy for constraints related to data of a user in a communication system; receive a request for data associated with the user from a service provider in the communication system, wherein the service provider possesses a privacy; check the request against a usage policy of the user; and decide whether the data can be released, wherein the privacy policy and the usage policy specify a strictness level, selected from a defined list of strictness levels, describing the constraints related to the access of data (figs. 2 and 3; paragraphs 84, 85, 115 and 175); wherein the components are configured to: permit the user to define the usage policy for the constraints related to the data (paragraphs 86-89); wherein the components are configured to: receive a predefined set of privacy policies and usage policies (paragraph 89); wherein receiving the predefined set comprises receiving the privacy policies and the usage policies comprising similar information elements (paragraph 89); wherein receiving the predefined set comprises receiving at least one of the privacy policies and at least one of the usage policies which specify a strictness level describing the constraints related to the data (paragraphs 85 and 175); wherein the components are configured to: permit the user to choose the usage policies for the constraints related to the data (paragraphs 86-89); wherein the components are configured to: release user

data when the at least one of the privacy policies of the service provider matches with the specified strictness level of the at least one of the usage policies of the user (paragraphs 117-126); wherein the components are configured to: allow the user to reduce a usage policy requirement when the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage policies of the user (paragraph 127)

13. Claims 1-8, 11-15 and 18-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Bohrer et al. US 2003/0088520 (hereinafter Bohrer).

14. As per claims 1-8, Bohrer discloses a method comprising:

j. receiving at a broker a usage policy for constraints related to data of a user in a communication system; receiving a request for data associated with the user from a service provider in the communication system to the broker, wherein the service provider possesses a privacy policy; checking, in the broker, the request against a usage policy of the user; and deciding whether the data can be released; (paragraphs 31, 83-87 and 89, "A trusted third party acts as a Personal Data Service (PDS) 804 for the Data Subject 800 ... A Data Requester 808 must also have a minimal set of software components 809 such as a local policy publisher and manager for the data requester's privacy policies stored in its policy repository 810 ... The Data Subject may choose to keep art of the Profile and Privacy policies on his own personal system as well ... Using the various software components 805, as described earlier in FIG.1 and elsewhere, the PDS

then authenticates the requester and matches the privacy policies of the requester with the authorization rules/privacy preference rules specified by the Data Subject.", figs. 1 and 8, reference nos. 804 and 805);

k. wherein the privacy policy and the usage policy specify a strictness level, selected from a defined list of strictness levels, describing the constraints related to the access of data; (paragraphs 49-76)

l. further comprising: using the user to define the usage policy for the constraints related to the data; (fig. 8, reference no. 801)

m. further comprising: providing the broker with a predefined set of privacy policies and usage policies; (paragraph 89)

n. wherein the providing comprises providing the privacy policies and the usage policies comprising similar information elements; (fig. 8, reference no. 805, "Policy Authorization Engine"; paragraph 49 utilizes p3p standard)

o. wherein the providing comprises providing at least one of the privacy policies and at least one of the usage policies which specify a strictness level describing the constraints related to the data; (figs 2 and 3 and related text)

p. further comprising: using the user to choose the usage policies for the constraints related to the data; (fig. 8, reference no. 801)

q. further comprising: releasing user data when the at least one of the privacy policies of the service provider matches with the specified strictness level of the at least one of the usage policies of the user; (paragraph 89, PDS

"matches the privacy policies of the requesters with the authorization rules/privacy preference rules specified by the Data Subject.")

r. further comprising: indicating, by the broker, the strictness level of the at least one of the usage policies of the user to the service provider when the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage policies of the user (paragraph 81).

15. As per claim 11, Bohrer discloses a system comprising: a service provider possessing a privacy policy; and a broker hosting a usage policy for constraints related to data of a user, configured to check a request from the service provider against the usage policy of the user and to decide whether data associated with the user can be released in response to the request; wherein the usage policy specify a strictness level, selected from a defined list of strictness levels, describing the constraints related to the access of data. (paragraphs 31, 49-76, 83-87 and 89, "A trusted third party acts as a Personal Data Service (PDS) 804 for the Data Subject 800 ... A Data Requester 808 must also have a minimal set of software components 809 such as a local policy publisher and manager for the data requester's privacy policies stored in its policy repository 810 ... The Data Subject may choose to keep art of the Profile and Privacy policies on his own personal system as well ... Using the various software components 805, as described earlier in FIG.1 and elsewhere, the PDS then authenticates the requester and matches the privacy policies of the requester with the authorization

rules/privacy preference rules specified by the Data Subject.", figs. 1 and 8, reference nos. 804 and 805).

16. As per claim 12, Bohrer discloses a system, comprising: introducing means for introducing to a broker a usage policy for constraints related to data of a user; receiving means for receiving a request for data associated with the user from a service provider to the broker; checking means for checking, in the broker, the request against a usage policy of the user; and deciding means for deciding whether the data can be released; wherein the usage policy specifies a strictness level, selected from a defined list of strictness levels, describing the constraints related to the access of data. (paragraphs 31, 49-76, 83-87 and 89, "A trusted third party acts as a Personal Data Service (PDS) 804 for the Data Subject 800 ... A Data Requester 808 must also have a minimal set of software components 809 such as a local policy publisher and manager for the data requester's privacy policies stored in its policy repository 810 ... The Data Subject may choose to keep art of the Profile and Privacy policies on his own personal system as well ... Using the various software components 805, as described earlier in FIG.1 and elsewhere, the PDS then authenticates the requester and matches the privacy policies of the requester with the authorization rules/privacy preference rules specified by the Data Subject.", figs. 1 and 8, reference nos. 804 and 805).

17. As per claims 13-15, Bohrer discloses an apparatus, comprising:

s. a receiver configured to receive a request for data associated with a user from a service provider; and a processor configured to check the request against a usage policy of the user and to decide whether the data can be released wherein the usage policy specifies a strictness level, selected from a defined list of strictness levels, describing constraints related to the access of data; (paragraphs 31, 49-76, 83-87 and 89, "A trusted third party acts as a Personal Data Service (PDS) 804 for the Data Subject 800 ... A Data Requester 808 must also have a minimal set of software components 809 such as a local policy publisher and manager for the data requester's privacy policies stored in its policy repository 810 ... The Data Subject may choose to keep art of the Profile and Privacy policies on his own personal system as well ... Using the various software components 805, as described earlier in FIG.1 and elsewhere, the PDS then authenticates the requester and matches the privacy policies of the requester with the authorization rules/privacy preference rules specified by the Data Subject.", figs. 1 and 8, reference nos. 804 and 805).

t. wherein the processor is further configured to: release user data when at least one privacy policy of the service provider matches with a specified strictness level of the usage policy of the user; (paragraph 89, PDS "matches the privacy policies of the requesters with the authorization rules/privacy preference rules specified by the Data Subject.")

u. wherein the processor is further configured to: indicate the strictness level of the at least one of the usage policies of the user to the service provider when

the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage policies of the user. (paragraph 81)

18. As per claim 18, Bohrer discloses an apparatus, comprising: receiving means for receiving a request for data associated with a user from a service provider; checking means for checking the request against a usage policy of the user; and deciding means for deciding whether the data can be released; wherein the usage policy specifies a strictness level, selected from a defined ordered list of strictness levels, describing the constraints related to the access of data. (paragraphs 31, 49-76, 83-87 and 89, "A trusted third party acts as a Personal Data Service (PDS) 804 for the Data Subject 800 ... A Data Requester 808 must also have a minimal set of software components 809 such as a local policy publisher and manager for the data requester's privacy policies stored in its policy repository 810 ... The Data Subject may choose to keep art of the Profile and Privacy policies on his own personal system as well ... Using the various software components 805, as described earlier in FIG.1 and elsewhere, the PDS then authenticates the requester and matches the privacy policies of the requester with the authorization rules/privacy preference rules specified by the Data Subject.", figs. 1 and 8, reference nos. 804 and 805).

19. As per claims 19-26, Bohrer discloses a computer-readable medium-comprising computer-executable components the components configured to:

v. receive a usage policy for constraints related to data of a user in a communication system; receive a request for data associated with the user from a service provider in the communication system, wherein the service provider possesses a privacy; check the request against a usage policy of the user; and decide whether the data can be released, wherein the privacy policy and the usage policy specify a strictness level, selected from a defined list of strictness levels, describing the constraints related to the access of data; (paragraphs 31, 49-76, 83-87 and 89, "A trusted third party acts as a Personal Data Service (PDS) 804 for the Data Subject 800 ... A Data Requester 808 must also have a minimal set of software components 809 such as a local policy publisher and manager for the data requester's privacy policies stored in its policy repository 810 ... The Data Subject may choose to keep art of the Profile and Privacy policies on his own personal system as well ... Using the various software components 805, as described earlier in FIG.1 and elsewhere, the PDS then authenticates the requester and matches the privacy policies of the requester with the authorization rules/privacy preference rules specified by the Data Subject.", figs. 1 and 8, reference nos. 804 and 805)

w. wherein the components are configured to: permit the user to define the usage policy for the constraints related to the data; (fig. 8, reference no. 801)

x. wherein the components are configured to: receive a predefined set of privacy policies and usage policies; (paragraph 89)

y. wherein receiving the predefined set comprises receiving the privacy policies and the usage policies comprising similar information elements; (fig. 8, reference no. 805, "Policy Authorization Engine"; paragraph 49 utilizes p3p standard)

z. wherein receiving the predefined set comprises receiving at least one of the privacy policies and at least one of the usage policies which specify a strictness level describing the constraints related to the data; (figs 2 and 3 and related text)

aa. wherein the components are configured to: permit the user to choose the usage policies for the constraints related to the data; (fig. 8, reference no. 801)

bb. wherein the components are configured to: release user data when the at least one of the privacy policies of the service provider matches with the specified strictness level of the at least one of the usage policies of the user; (paragraph 89, PDS "matches the privacy policies of the requesters with the authorization rules/privacy preference rules specified by the Data Subject.")

cc. wherein the components are configured to: indicate the strictness level of the at least one of the usage policies of the user to the service provider when the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage policies of the user. (paragraph 81)

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 9, 16 and 27 are rejected under 35 USC 103(a) as being unpatentable over Bohrer in view of Koike.

22. As per claim 9, the rejection of claim 5 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not expressly disclose allowing the user to reduce a usage policy requirement when the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage policies of the user. Koike discloses a method for administrating data including privacy of a user in communication made between a server and the user's terminal device, whereby user privacy data is provided when the privacy policies of the server matches the usage policy requirement of the user (paragraphs 115-127); moreover, the invention of Koike also provides a override feature, wherein if the privacy policies of the server does not match the usage policy requirement of the user, the user can still allow the privacy data to be sent to the server. (paragraph 127) It would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Bohrer to further include the feature of allowing the user to reduce a usage policy requirement when the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage

policies of the user. One would be motivated to do so to provide more flexibility for a user to determine when privacy information is to be sent to a service provider as known to one of ordinary skill in the art and as suggested by Koike. The aforementioned cover the limitations of claim 9.

23. As per claim 16, the rejection of claim 13 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not expressly disclose the processor is further configured to allow the user to reduce a usage policy requirement when the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage policies of the user. Koike discloses a method for administrating data including privacy of a user in communication made between a server and the user's terminal device, whereby user privacy data is provided when the privacy policies of the server matches the usage policy requirement of the user (paragraphs 115-127); moreover, the invention of Koike also provides a override feature, wherein if the privacy policies of the server does not match the usage policy requirement of the user, the user can still allow the privacy data to be sent to the server. (paragraph 127) It would be obvious to one of ordinary skill in the art at the time the invention was made wherein the processor is further configured to allow the user to reduce a usage policy requirement when the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage policies of the user. One would be motivated to do so to provide more flexibility for a user to determine when privacy information is to be sent to a service

provider as known to one of ordinary skill in the art and as suggested by Koike. The aforementioned cover the limitations of claim 16.

24. As per claim 27, the rejection of claim 23 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not expressly disclose the components are further configured to allow the user to reduce a usage policy requirement when the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage policies of the user. Koike discloses a method for administrating data including privacy of a user in communication made between a server and the user's terminal device, whereby user privacy data is provided when the privacy policies of the server matches the usage policy requirement of the user (paragraphs 115-127); moreover, the invention of Koike also provides a override feature, wherein if the privacy policies of the server does not match the usage policy requirement of the user, the user can still allow the privacy data to be sent to the server. (paragraph 127) It would be obvious to one of ordinary skill in the art at the time the invention was made wherein the components are further configured to allow the user to reduce a usage policy requirement when the at least one of the privacy policies of the service provider does not match with the specified strictness level of the at least one of the usage policies of the user. One would be motivated to do so to provide more flexibility for a user to determine when privacy information is to be sent to a service provider as known to one of ordinary skill in the art and as suggested by Koike. The aforementioned cover the limitations of claim 27.

25. Claims 10, 17 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koike in view of Holtmanns et al. US 2005/0086061 (hereinafter Holtmanns).

26. As per claim 10, the rejection of claim 1 under 35 USC 102(e) as being anticipated by Koike is incorporated herein. Koike does not disclose attaching an electronically signed usage policy to the data when the data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the communications server to protect the user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Koike to further include the step of attaching an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the communications server from modification of the privacy policy by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 10.

27. As per claim 17, the rejection of claim 13 under 35 USC 102(e) as being anticipated by Koike is incorporated herein. Koike does not disclose the processor is further configured to attach an electronically signed usage policy to the data when the

data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the communications server to protect the user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the processor of Koike to be further configured to attach an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the communications server from modification of the privacy policy by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 17.

28. As per claim 28, the rejection of claim 23 under 35 USC 102(e) as being anticipated by Koike is incorporated herein. Koike does not disclose the components are further configured to attach an electronically signed usage policy to the data when the data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the communications server to protect the user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it

would be obvious to one of ordinary skill in the art at the time the invention was made for the components of Koike to be further configured to attach an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the communications server from modification of the privacy policy by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 28.

29. Claims 10, 17 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bohrer in view of Holtmanns et al. US 2005/0086061 (hereinafter Holtmanns).

30. As per claim 10, the rejection of claim 1 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not disclose attaching an electronically signed usage policy to the data when the data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the communications server to protect the user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Bohrer to further include the step of attaching an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the

communications server from modification of the privacy policy by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 10.

31. As per claim 17, the rejection of claim 13 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not disclose the processor is further configured to attach an electronically signed usage policy to the data when the data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the communications server to protect the user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the processor of Bohrer to be further configured to attach an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the communications server from modification of the privacy policy by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 17.

32. As per claim 28, the rejection of claim 23 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not disclose the components are further configured to attach an electronically signed usage policy to the data when

the data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the communications server to protect the user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the components of Bohrer to be further configured to attach an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the communications server from modification of the privacy policy by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 28.

Conclusion

33. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See enclosed PTO-892.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2132